Singly-even self-dual codes with minimal shadow

Stefka Bouyuklieva* and Wolfgang Willems

Faculty of Mathematics, University of Magdeburg
39016 Magdeburg, Germany

Abstract

In this note we investigate extremal singly-even self-dual codes with minimal shadow. For particular parameters we prove non-existence of such codes. By a result of Rains [11], the length of extremal singly-even self-dual codes is bounded. We give explicit bounds in case the shadow is minimal.

Index Terms: *self-dual codes, singly-even codes, minimal shadow, bounds*

1 Introduction

Let C be a singly-even self-dual $[n, \frac{n}{2}, d]$ code and let C_0 be its doubly-even subcode. There are three cosets C_1, C_2, C_3 of C_0 such that $C_0^\perp = C_0 \cup C_1 \cup C_2 \cup C_3$, where $C = C_0 \cup C_2$. The set $S = C_1 \cup C_3 = C_0^\perp \setminus C$ is called the shadow of C. Shadows for self-dual codes were introduced by Conway and Sloane [5] in order to derive new upper bounds for the minimum weight of singly-even self-dual codes and to provide restrictions on their weight enumerators.

According to [10] the minimum weight d of a self-dual code of length n is bounded by $4[n/24] + 4$ for $n \not\equiv 22 \pmod{24}$ and by $4[n/24] + 6$ if $n \equiv 22 \pmod{24}$. We call a self-dual code meeting this bound extremal. Note that for some lengths, for instance length 34, no extremal self-dual codes exist.

Some properties of the weight enumerator of S are given in the following theorem.

Theorem 1 [5] *Let $S(y) = \sum_{r=0}^{n} B_r y^r$ be the weight enumerator of S. Then*

- $B_r = B_{n-r}$ *for all* r,
- $B_r = 0$ *unless* $r \equiv n/2 \pmod 4$,
- $B_0 = 0$,

*Supported by the Humboldt Foundation. On leave from Faculty of Mathematics and Informatics, Veliko Tarnovo University, 5000 Veliko Tarnovo, Bulgaria

- $B_r \leq 1$ *for* $r < d/2$,
- $B_{d/2} \leq 2n/d$,
- *at most one* B_r *is nonzero for* $r < (d+4)/2$.

Elkies studied in [6] the minimum weight s (respectively the minimum norm) of the shadow of self-dual codes (respectively of unimodular lattices), especially in the cases where it attains a high value. Bachoc and Gaborit proposed to study the parameters d and s simultaneously [1]. They proved that $2d + s \leq \frac{n}{2} + 4$, except in the case $n \equiv 22 \pmod{24}$ where $2d + s \leq \frac{n}{2} + 8$. They called the codes attaining this bound *s-extremal*. In this note we study singly-even self-dual codes for which the minimum weight of the shadow has smallest possible value. possible.

Definition 1 *We say that a self-dual code* C *of length* $24m + 8l + 2r$ *with* $r = 1, 2, 3$ *and* $l = 0, 1, 2$ *is a code with minimal shadow if* $\mathrm{wt}(S) = r$. *For* $r = 0$, C *is called of minimal shadow if* $\mathrm{wt}(S) = 4$.

Self-dual codes with minimal shadow are subject of two previous articles. The paper [3] is devoted to connections between self-dual codes of length $24m + 8l + 2$ with $\mathrm{wt}(S) = 1$, combinatorial designs and secret sharing schemes. The structure of these codes are used to characterize access groups in a secret sharing scheme based on codes. There are two types of schemes which are proposed - with one-part secret and with two-part secret. Moreover, some of the considered codes support 1- and 2-designs. The performance of the extremal self-dual codes of length $24m + 8l$ where $l = 1, 2$ have been studied in [2]. In particular, different types of codes with the same parameters are compared with regard to the decoding error probability. It turned out that for lengths $24m+8$ singly-even codes with minimal shadow perform better than doubly-even codes. Thus from the point of view of data correction one is interested in singly-even codes with minimal shadow.

This article is organized as follows. In Section 2 we prove that extremal self-dual codes with minimal shadow of length $24m + 2t$ for $t = 1, 2, 3, 5, 11$ do not exist. Moreover, for $t = 4, 6, 7$ and 9, we obtain upper bounds for the length. We also prove that if extremal doubly-even self-dual codes of length $n = 24m + 8$ or $24m + 16$ do not exist then extremal singly-even self-dual codes with minimal shadow do not exist for the same length. The only case for which we do not have a bound for the length is $n = 24m + 20$.

All computations have been carried out with Maple.

2 Extremal self-dual codes with minimal shadow

Let C be a singly-even self-dual code of length $n = 24m + 8l + 2r$ where $l = 0, 1, 2$ and $r = 0, 1, 2, 3$. The weight enumerator of C and its shadow are given by [5]:

$$W(y) = \sum_{j=0}^{12m+4l+r} a_j y^{2j} = \sum_{i=0}^{3m+l} c_i (1+y^2)^{12m+4l+r-4i} (y^2(1-y^2)^2)^i$$

$$S(y) = \sum_{j=0}^{6m+2l} b_j y^{4j+r} = \sum_{i=0}^{3m+l} (-1)^i c_i 2^{12m+4l+r-6i} y^{12m+4l+r-4i} (1-y^4)^{2i}$$

Using these expressions we can write c_i as a linear combination of the a_j and as a linear combination of the b_j in the following way [10]:

$$c_i = \sum_{j=0}^{i} \alpha_{ij} a_j = \sum_{j=0}^{3m+l-i} \beta_{ij} b_j. \tag{1}$$

Suppose C is an extremal singly-even self-dual code with minimal shadow, hence $d = 4m + 4$ and $\mathrm{wt}(S) = r$ if $r = 1, 2, 3$ and $\mathrm{wt}(S) = 4$ if $r = 0$. Obviously in this case $a_0 = 1$, $a_1 = a_2 = \cdots = a_{2m+1} = 0$. According to Theorem 1, we have $b_0 = 1$ if $r > 0$ and $m \geq 1$, and $b_0 = 0, b_1 = 1$ if $r = 0$ and $m \geq 2$.

Moreover, if $r > 0$ and $m \geq 1$ then $b_1 = b_2 = \cdots = b_{m-1} = 0$. Otherwise S would contain a vector v of weight less than or equal to $4m - 4 + r$, and if $u \in S$ is a vector of weight r then $u + v \in C$ with $\mathrm{wt}(u + v) \leq 4m + 2r - 4 \leq 4m + 2$, a contradiction to the minimum distance of C. Similarly, if $r = 0$ and $m \geq 2$ then $b_2 = \cdots = b_{m-1} = 0$.

Remark 1 For extremal self-dual codes of length $24m + 8l + 2$ we furthermore have $b_m = 0$. Otherwise S would contain a vector v of weight $4m + 1$, and if $u \in S$ is the vector of weight 1 which exists since $\mathrm{wt}(S) = 1$, then $u+v \in C$ with $\mathrm{wt}(u+v) \leq 4m+2$ contradicting the minimum distance of C.

If $m \geq 2$ we have by (1)

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,\epsilon} + \sum_{j=m}^{m+l-1} \beta_{2m+1,j} b_j, \tag{2}$$

where $\epsilon = 1$ for $r = 0$ and $\epsilon = 0$ otherwise, since $3m+l-2m-1 = m+l-1$. To evaluate this equation, which turns out to be crucial in the following, we need to consider the coefficients α_{i0} in details. In order to do this we denote by $\alpha_i(n)$ the coefficient α_{i0} if n is the length of the code. According to [10] we have

$$\alpha_i(n) = \alpha_{i0} = -\frac{n}{2i}[\text{coeff. of } y^{i-1} \text{ in } (1+y)^{-n/2-1+4i}(1-y)^{-2i}]. \tag{3}$$

Let $t = 4l + r$ and $n = 24m + 8l + 2r = 24m + 2t$. Then

$$\begin{aligned}\alpha_{2m+1}(n) &= -\frac{12m+t}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1+y)^{-12m-t-1+8m+4}(1-y)^{-4m-2}] \\ &= -\frac{12m+t}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1+y)^{-4m-t+3}(1-y)^{-4m-2}]\end{aligned}$$

For $t > 5$ we obtain

$$\alpha_{2m+1}(n) = -\frac{12m+t}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1-y^2)^{-4m-t+3}(1-y)^{t-5}],$$

and if $t \leq 5$ then

$$\alpha_{2m+1}(n) = -\frac{12m+t}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1-y^2)^{-4m-2}(1+y)^{5-t}].$$

Since

$$(1-y^2)^{-a} = \sum_{0 \leq j} \binom{-a}{j}(-1)^j y^{2j} = \sum_{0 \leq j} \binom{a+j-1}{j} y^{2j} \quad \text{for } a > 0,$$

it follows in case $t \leq 5$ that

$$\begin{aligned}\alpha_{2m+1}(n) &= -\frac{12m+t}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1+y)^{5-t} \sum_{j=0}^{m} \binom{4m+j+1}{j} y^{2j}] \\ &= -\frac{12m+t}{2m+1} \sum_{s=0}^{[\frac{5-t}{2}]} \binom{5-t}{2s} \binom{5m+1-s}{m-s},\end{aligned}$$

and in case $t > 5$ that

$$\begin{aligned}\alpha_{2m+1}(n) &= -\frac{12m+t}{2m+1}[\text{coeff. of } y^{2m} \text{ in } (1-y)^{t-5} \sum_{j=0}^{m} \binom{4m+t+j-4}{j} y^{2j}] \\ &= -\frac{12m+t}{2m+1} \sum_{s=0}^{[\frac{t-5}{2}]} \binom{t-5}{2s} \binom{5m+t-4-s}{m-s}.\end{aligned}$$

For the different lengths n the values of $\alpha_{2m+1}(n)$ are listed in Table 1.

To evaluate equation (2) we also need β_{ij} which are known due to [10]. Here we have

$$\beta_{ij} = (-1)^i 2^{-n/2+6i} \frac{k-j}{i} \binom{k+i-j-1}{k-i-j}, \tag{4}$$

Table 1: The values $\alpha_{2m+1}(n)$ for extremal self-dual codes

n	$24m+2$	$24m+10$	$24m+18$
α_{2m+1}	$-\frac{(12m+1)(56m+4)}{(2m+1)(m-1)}\binom{5m-1}{m-2}$	$-\frac{12m+5}{2m+1}\binom{5m+1}{m}$	$-\frac{12(7m+5)(4m+3)}{m(m-1)}\binom{5m+3}{m-2}$
n	$24m+4$	$24m+12$	$24m+20$
α_{2m+1}	$-\frac{2(6m+1)(8m+1)}{m(2m+1)}\binom{5m}{m-1}$	$-6\binom{5m+2}{m}$	$-\frac{20(6m+5)(4m+3)}{m(m-1)}\binom{5m+4}{m-2}$
n	$24m+6$	$24m+14$	$24m+22$
α_{2m+1}	$-\frac{3(4m+1)(6m+1)}{m(2m+1)}\binom{5m}{m-1}$	$-\frac{3(12m+7)}{m}\binom{5m+2}{m-1}$	$-\frac{6(12m+11)(6m+5)(8m+7)}{m(m-1)(m-2)}\binom{5m+4}{m-3}$
n	$24m+8$	$24m+16$	
α_{2m+1}	$-\frac{4(3m+1)}{2m+1}\binom{5m+1}{m}$	$-\frac{16(3m+2)}{m}\binom{5m+3}{m-1}$	

where $k = \lfloor n/8 \rfloor = 3m + l$. In particular,

$$\beta_{2m+1,j} = -2^{6-t}\frac{3m+l-j}{2m+1}\binom{5m+l-j}{m+l-1-j} \quad \text{and} \quad \beta_{2m+1,m+l-1} = -2^{6-t}.$$

Now we are prepared to prove:

Theorem 2 *Extremal self-dual codes of lengths $n = 24m+2$, $24m+4$, $24m+6$, $24m+10$ and $24m+22$ with minimal shadow do not exist.*

Proof. According to [10] any extremal self-dual code of length $24m+22$ has minimum distance $4m+6$ and the minimum weight of its shadow is $4m+7$. Thus the shadow is not minimal since a minimal shadow must have minimum weight 3. (There is a misprint in [10] where it is stated that the minimum weight of the shadow is $4m+6$. But actually the weights in this shadow are of type $4j+3$).

In the other four cases we have

$$c_{2m+1} = \alpha_{2m+1,0} = \beta_{2m+1,0} \tag{5}$$

by (2). In case $n = 24m+10$ we use the fact that $b_m = 0$, according to Remark 1.

Simplifying equation (5) according to Table 1 we obtain

$$\begin{aligned} 48m^2 + 26m + 1 = 0, &\quad \text{if } n = 24m+2 \\ 24m^2 + 14m + 1 = 0, &\quad \text{if } n = 24m+4 \\ 48m^2 + 30m + 3 = 0, &\quad \text{if } n = 24m+6 \\ 6m + 3 = 0, &\quad \text{if } n = 24m+10. \end{aligned}$$

Since all these equations have no solutions $m \geq 0$ extremal self-dual codes with minimal shadow do not exist for $n \equiv 2, 4, 6, 10 \bmod 24$. $\square$

Remark 2 So far no extremal self-dual codes of length $24m + 2t$ are known for $t = 1, 2, 3, 5$. According to [8] extremal self-dual codes of length $24m + 2r$ do not exist for $r = 1, 2, 3$ and $m = 1, 2, \ldots, 6, 8, \ldots, 12, 16, \ldots, 22$. Thus if there is (for instance) a self-dual $[170, 85, 32]$ code it will not have minimal shadow, by Theorem 2.

The next result is a crucial observation in order to prove explicit bounds for the existence of extremal singly-even self-dual codes.

Theorem 3 *Extremal singly-even self-dual codes with minimal shadow of lengths* $n = 24m+8$, $24m+12$, $24m+14$ *and* $24m+18$ *have uniquely determined weight enumerators.*

Proof. For $m = 0$ and $m = 1$ see Remark 3 and the examples at the end of the paper. Now let $m \geq 2$.

In case $n = 24m + 12$ or $n = 24m + 14$ we have

$$c_i = \alpha_{i0} = \beta_{i0} + \sum_{j=m}^{3m+1-i} \beta_{ij} b_j \quad \text{for } i \leq 2m+1 \quad \text{and}$$

$$c_i = \alpha_{i0} + \sum_{j=2m+2}^{i} \alpha_{ij} a_j = \beta_{i0} \quad \text{for } i > 2m+1.$$

Therefore $c_i = \alpha_{i0}$ for $i = 0, 1, \ldots, 2m+1$ and $c_i = \beta_{i0}$ for $i = 2m+2, \ldots, 3m+1$.

In the case $n = 24m + 8$ we have $b_0 = 0$, $b_1 = 1$ and $b_2 = \cdots = b_{m-1} = 0$. Hence $c_i = \alpha_{i0}$ for $i = 0, 1, \ldots, 2m+1$ and $c_i = \beta_{i1}$ for $i = 2m+2, \ldots, 3m+1$.

Similarly, if $n = 24m + 18$ we obtain $c_i = \alpha_{i0}$ for $i = 0, 1, \ldots, 2m+1$ and $c_i = \beta_{i0}$ for $i = 2m+2, \ldots, 3m+2$. In both cases the weight enumerator can be computed as above.

By (3) and (4), the values of c_i can be calculated and they depend only on the length n. Thus the weight enumerators are unique in all cases. $\square$

In [15], Zhang obtained upper bounds for the lengths of the extremal binary doubly-even codes. He proved that extremal doubly-even codes of length $n = 24m + 8l$ do not exist if $m \geq 154$ (for $l = 0$), $m \geq 159$ (for $l = 1$) and $m \geq 164$ (for $l = 2$). For extremal singly-even codes there is also a bound due to Rains [11]. Unfortunately, he only states the existence of a bound. In the next corollary we give explicit bounds for extremal singly-even self-dual codes with minimal shadow for lengths congruent 8, 12, 14 and 18 mod 24.

In the proof we need the value of $c_{2m} = \alpha_{2m,0}$. According to [10] we have

$$\begin{aligned}
\alpha_{2m}(n) &= -\frac{24m+2t}{4m}[\text{coeff. of } y^{2m-1} \text{ in } (1+y)^{-4m-t-1}(1-y)^{-4m}] \\
&= -\frac{12m+t}{2m}[\text{coeff. of } y^{2m-1} \text{ in } (1-y)^{t+1}(1-y^2)^{-4m-t-1}] \\
&= -\frac{12m+t}{2m}[\text{coeff. of } y^{2m-1} \text{ in } (1-y)^{t+1}\sum_{j=0}^{m}\binom{4m+t+j}{j}y^{2j}] \\
&= \frac{12m+t}{2m}\sum_{s=1}^{[\frac{t+2}{2}]}\binom{t+1}{2s-1}\binom{5m+t-s}{m-s}
\end{aligned}$$

where $t = 4l + r$ and $n = 24m + 8l + 2r = 24m + 2t$. The values for $\alpha_{2m}(n)$ are listed in Table 2.

Table 2: The values $\alpha_{2m}(n)$ for an extremal self-dual $[n = 24m + 2t, \frac{n}{2}, 4m + 4]$ code

n	$\alpha_{2m}(n)$
$24m+8$	$\frac{8(4m+1)(11m+3)(3m+1)}{m(m-1)(m-2)}\binom{5m+1}{m-3}$
$24m+12$	$\frac{24(116m^2+79m+15)(1+2m)^2}{m(m-1)(m-2)(m-3)}\binom{5m+2}{m-4}$
$24m+14$	$\frac{24(1+2m)(12m+7)(28m^2+22m+5)}{m(m-1)(m-2)(m-3)}\binom{5m+3}{m-4}$
$24m+16$	$\frac{16(3m+2)(2m+1)(1216m^3+1956m^2+1073m+210)}{m(m-1)(m-2)(m-3)(m-4)}\binom{5m+3}{m-5}$
$24m+18$	$\frac{120(2m+1)(4m+3)(176m^3+308m^2+189m+42)}{m(m-1)(m-2)(m-3)(m-4)}\binom{5m+4}{m-5}$
$24m+20$	$\frac{16(6m+5)(2m+1)(4m+3)(1592m^3+3280m^2+2363m+630)}{m(m-1)(m-2)(m-3)(m-4)(m-5)}\binom{5m+4}{m-6}$

Furthermore, $\beta_{2m,j} = 2^{-t}\frac{3m+l-j}{2m}\binom{5m+l-1-j}{m+l-j}$. Hence $\beta_{2m,m+l} = 2^{-t}$ and $\beta_{2m,m+l-1} = 2^{1-t}(2m+1)$.

Corollary 4 *There are no extremal singly-even self-dual codes of length n with minimal shadow if*

(i) $n = 24m + 8$ *and* $m \geq 53$,

(ii) $n = 24m + 12$ *and* $m \geq 142$,

(iii) $n = 24m + 14$ *and* $m \geq 146$,

(iv) $n = 24m + 18$ *and* $m \geq 157$.

Proof. Using the equation

$$c_i = \alpha_{i0} = \beta_{i\epsilon} + \sum_{j=m}^{3m+l-i} \beta_{ij} b_j \quad \text{for } i \leq 2m+1,$$

where $\epsilon = 1$ if $n = 24m + 8$ and $\epsilon = 0$ in the other cases, we see that

$$b_{m+l-1} = -2^{t-6}(\alpha_{2m+1,0} - \beta_{2m+1,\epsilon}).$$

The values of b_m for $n = 24m + 8$, $24m + 12$ and $24m + 14$ are given in Table 3.

Table 3: The parameter b_m for extremal self-dual codes of length n

n	$24m+8$	$24m+12$	$24m+14$
b_m	$\frac{6m+1}{m}\binom{5m}{m-1}$	$\frac{12m+5}{2m+1}\binom{5m+1}{m}$	$\frac{168m^2+164m+39}{(2m+1)(4m+3)}\binom{5m+1}{m}$

If $n = 24m + 18$ we have

$$b_m = 0 \quad \text{and} \quad b_{m+1} = \frac{(24m+17)(17m+10)}{(2m+1)(4m+5)}\binom{5m+2}{m+1}.$$

In the first three cases we compute

$$b_{m+1} = \frac{\alpha_{2m,0} - \beta_{2m,\epsilon} - \beta_{2m,m} b_m}{\beta_{2m,m+1}}.$$

If $n = 24m + 8$ we obtain

$$b_{m+1} = \frac{16(6m+1)(-4m^3+209m^2+141m+24)}{5m(m+1)(4m+3)}\binom{5m+1}{m-1}$$

In case $m \geq 53$ the polynomial $-4m^3 + 209m^2 + 141m + 24$ takes negative values, hence $b_{m+1} < 0$, a contradiction.

For $24m + 12$ we have

$$b_{m+1} = \frac{2(12m+5)(-32m^4+4496m^3+4242m^2+1257m+117)}{(5m+1)(4m+3)(4m+5)(2m+3)}\binom{5m+2}{m+1}$$

If $m \geq 142$ the polynomial $-32m^4 + 4496m^3 + 4242m^2 + 1257m + 117$ takes negative values, hence $b_{m+1} < 0$, a contradiction.

For $24m+14$ the calculations lead to

$$b_{m+1} = \frac{2(-5376m^6+772352m^5+1663728m^4+1386448m^3+557970m^2+107643m+7875)}{(4m+3)(4m+5)(2m+3)(4m+7)(5m+1)}\binom{5m+2}{m+1}$$

which is negative if $m \geq 146$.

In the last case we have to compute

$$b_{m+2} = \frac{\alpha_{2m,0} - \beta_{2m,0} - \beta_{2m,m+1}b_{m+1}}{\beta_{2m,m+2}}.$$

The computations yield

$$b_{m+2} = \frac{2(24m+17)(-544m^5+83696m^4+184210m^3+149089m^2+52809m+6930)}{(4m+5)(2m+3)(4m+7)(4m+9)(5m+2)}\binom{5m+3}{m+2}$$

which is negative for $m \geq 157$. □

Proposition 5 *If there are no extremal doubly-even self-dual codes of length $n = 24m+8$ or $24m+16$ then there are no extremal singly-even self-dual codes of length n with minimal shadow.*

Proof. We shall prove the contraposition. Let C be a singly-even self-dual $[n = 24m+8l, 12m+4l, 4m+4]$ code and suppose that the coset C_1 contains the vector u of weight 4. If $v \in C_3$ then $u+v \in C_2$ and hence $\mathrm{wt}(u+v) \geq 4m+6$. It follows that

$$\mathrm{wt}(v) \geq 4m+6-4+2\mathrm{wt}(u*v) \geq 4m+4,$$

since C_1 is not orthogonal to C_3, which means that $u*v \equiv 1 \pmod 2$ for $u \in C_1, v \in C_3$ (see [4]). Thus $\mathrm{wt}(C_3) \geq 4m+4$. Therefore $C_0 \cup C_3$ is an extremal doubly-even code with parameters $[24m+8l, 12m+4l, 4m+4]$. □

Corollary 6 *There are no extremal singly-even self-dual codes with minimal shadow of length $n = 24m+16$ for $m \geq 164$.*

Proof. This follows immediately from the Zhang bound [15] for doubly-even codes in connection with Proposition 5. □

Summarizing the results in Theorem 2, Corollary 4 and Corollary 6 we have proved either the non-existence or an explicit bound for the length n of an extremal singly-even self-dual code unless $n \equiv 20 \pmod{24}$. To find an explicit bound for $n = 24m+20$ seems to be difficult since the weight enumerator is not unique in this case.

Remark 3 Extremal singly-even self-dual codes of length $24m + 8$ are constructed only for $m = 1$, i.e. $n = 32$. There are exactly three inequivalent singly-even self-dual $[32, 16, 8]$ codes. Yorgov proved that there are no extremal singly-even self-dual codes with minimal shadow of length $24m + 8$ in the case m is even and $\binom{5m}{m}$ is odd [14].

Examples. Extremal singly-even self-dual codes of lengths $24m + 12$, $24m + 14$ and $24m + 18$:

$m = 0$: There are unique extremal singly-even codes of lengths 12, 14 and 16, and they have minimal shadows. There are two inequivalent self-dual $[18, 9, 4]$ codes, but only one of them is a code with minimal shadow (see [5]).
$m = 1$: Extremal self-dual codes of lengths 36, 38 and 42 with minimal shadow are constructed. Only for the length 36 there is a complete classification [9]. There are 16 inequivalent self-dual $[36, 18, 8]$ codes with minimal shadow and their weight enumerator is $W = 1 + 225y^8 + 2016y^{10} + 9555y^{12} + \cdots$ (see [7]).
$m = 2$: There exists a doubly circulant code with parameters $[60, 30, 12]$ and shadow of minimum weight 2, denoted by $D13$ in [5]. The first examples for extremal self-dual codes with minimal shadow of lengths 62 and 66 are constructed in [12] and [13], respectively.

Finally, we would like to mention that similar to the case of extremal doubly-even self-dual codes there is a large gap between the bounds for extremal singly-even self-dual codes and what we really can construct.

References

[1] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory Ser. A*, **105** (2004), 15–34.

[2] S. Bouyuklieva, A. Malevich and W. Willems, On the performance of binary extremal self-dual codes, *Advances in Mathematics of Communications* **5** (2011), 267–274.

[3] S. Bouyuklieva and Z. Varbanov, Some connections between self-dual codes, combinatorial designs and secret sharing schemes, *Advances in Mathematics of Communications* **5** (2011), 191–198.

[4] R. Brualdi and V. Pless, Weight Enumerators of Self-Dual Codes, *IEEE Trans. Inform. Theory* **37** (1991), 1222–1225.

[5] J.H.Conway and N.J.A.Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory*, **36** (1990), 1319–1333.

[6] N. Elkies, Lattices and codes with longshadows, *Math. Res. Lett.* 2 (5) (1995), 643-651.

[7] C.A. Melchor and P. Gaborit, On the classification of extremal $[36, 18, 8]$ binary self-dual codes, *IEEE Trans. Inform. Theory*, **54** (2008), 4743–4750.

[8] S. Han and J.B. Lee, Nonexistence of some extremal self-dual codes, J. Korean Math. Soc. **43** (2006), No. 6, 1357-1369.

[9] W.C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields Appl.* **11** (2005), 451–490.

[10] E.M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), 134–139.

[11] E.M. Rains, New asymptotic bounds for self-dual codes and lattices, *IEEE Trans. Inform. Theory* **49** (2003), 1261–1274.

[12] R. Russeva and N. Yankov, On binary self-dual codes of lengths 60, 62, 64 and 66 having an automorphism of order 9, *Designs, Codes and Cryptography* **45** (2007), 335-346.

[13] H.P. Tsai, Extremal self-dual codes of length 66 and 68, *IEEE Trans. Inform. Theory* **45** (1999), 2129-2133.

[14] V. Yorgov, On the minimal weight of some singly-even codes, *IEEE Transactions on Information Theory* **45** (1999), 2539-2541.

[15] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277-286.